Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Number Theory 119 (2006) 210–241

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

On the number of incongruent residues of $x^4 + ax^2 + bx$ modulo p ☆

Zhi-Hong Sun

Department of Mathematics, Huaiyin Teachers College, Huaian, Jiangsu 223001, PR China

Received 1 December 2003; revised 26 September 2005

Available online 15 December 2005

Communicated by David Goss

Abstract

Let $p > 3$ be a prime and $a, b \in \mathbb{Z}$. In the paper we mainly determine the number $V_p(x^4 + ax^2 + bx)$ of incongruent residues of $x^4 + ax^2 + bx$ $(x \in \mathbb{Z})$ modulo p and reveal the connections with elliptic curves over the field $\mathbb{F}_p$ of p elements.

MSC: primary 11A07; secondary11A15, 11E25, 11L10, 14H52, 11Y11

Keywords: The number of incongruent residues; Quartic polynomial; Congruence; Elliptic curve

1. Introduction

Let $\mathbb{Z}$ be the set of integers. For a positive integer m and given polynomial $f(x)$ with integral coefficients, denote the number of incongruent residues of $f(x)$ $(x \in \mathbb{Z})$ modulo m by $V_m(f(x))$. That is,

$$V_m\big(f(x)\big) = \big|\big\{c\colon\ c \in \{0, 1, \ldots, m-1\},\ \ f(x) \equiv c \pmod m \text{ is solvable}\big\}\big|.$$

Let $p > 3$ be a prime, $a_1, a_2, a_3 \in \mathbb{Z}$, and let $(\frac{d}{p})$ be the Legendre symbol. In 1908 von Sterneck [St] proved that if $a_1^2 \not\equiv 3a_2 \pmod p$, then

☆ Research of the author was supported by Natural Sciences Foundation of Jiangsu Educational Office (02KJB110007).

E-mail address: hyzhsun@public.hy.js.cn.

URL: http://www.hytc.cn/xsjl/szh.

0022-314X/$ – see front matter

doi:10.1016/j.jnt.2005.10.012

$$V_p\big(x^3+a_1x^2+a_2x+a_3\big)=\frac{2p+(\frac{p}{3})}{3}. \tag{1.1}$$

This result was rediscovered by the author [Su1, Theorem 4.3]. See also [K,MW1]. In the paper we give a general result for $V_m(x^3+a_1x^2+a_2x+a_3)$, where m is a positive integer.

For the general quartic polynomial $x^4+a_1x^3+a_2x^2+a_3x+a_4$ let

$$a=16a_2-6a_1^2,\qquad b=8\big(8a_3-4a_1a_2+a_1^3\big),$$
$$c=256a_4-64a_1a_3+16a_1^2a_2-3a_1^4$$

and $X=4x+a_1$. Then we find

$$x^4+a_1x^3+a_2x^2+a_3x+a_4=\frac{1}{256}\big(X^4+aX^2+bX+c\big) \tag{1.2}$$

and so

$$V_p\big(x^4+a_1x^3+a_2x^2+a_3x+a_4\big)=V_p\big(x^4+ax^2+bx+c\big)=V_p\big(x^4+ax^2+bx\big). \tag{1.3}$$

Hence it suffices to discuss $V_p(x^4+ax^2+bx)$. In [MW2] McCann and Williams showed that

$$V_p\big(x^4+ax^2+bx\big)=\begin{cases}\frac{3}{8}p+O(1) & \text{if } p\nmid a \text{ and } p\mid b,\\ \frac{5}{8}p+O(\sqrt{p}) & \text{if } p\nmid b.\end{cases}$$

For a general estimate for $V_p(f(x))$ one may consult [BSD].

For $a,b,c\in\mathbb{Z}$ let

$$D(a,b,c)=-\big(4a^3+27b^2\big)b^2+16c\big(a^4+9ab^2-8a^2c+16c^2\big). \tag{1.4}$$

It is known that $D(a,b,c)$ is the discriminant of x^4+ax^2+bx+c and $x^3+2ax^2+(a^2-4c)x-b^2$. From [Sk,Leo] and [Su3, Theorem 5.8] we have the following basic result for quartic congruences.

Let $p>3$ be a prime, $a,b,c\in\mathbb{Z}$ and $p\nmid bD(a,b,c)$. Then

$$\begin{aligned}&x^4+ax^2+bx+c\equiv 0 \pmod p \quad\text{is unsolvable}\\ \iff\ &\text{there exists an integer } y \text{ such that } \left(\frac{y}{p}\right)=-1\\ &\text{and } y^3+2ay^2+\big(a^2-4c\big)y-b^2\equiv 0 \pmod p.\end{aligned} \tag{1.5}$$

On the basis of this result, in the paper we try to determine $V_p(x^4+ax^2+bx)$ $(a,b\in\mathbb{Z})$ for any prime $p>3$ and obtain some explicit formulas.

Let $[\alpha]$ denote the greatest integer not exceeding α. Let $\#E_p(x^3-Ax-B)$ be the number of points on the elliptic curve E_p: $y^2=x^3-Ax-B$ over the field $\mathbb{F}_p$ of p elements. We list the following typical results in the paper.

$$V_p\big(x^4-6x^2+8x\big)=\left[\frac{5p+7}{8}\right]. \tag{1.6}$$

$$\text{If } p\equiv 2 \pmod 3 \text{ and } p\nmid b, \quad \text{then } V_p\big(x^4+bx\big)=\left[\frac{5p+7}{8}\right]. \tag{1.7}$$

If $p\equiv 7 \pmod{12}$, $p\nmid b$ and $p=A^2+3B^2$ $(A,B\in\mathbb{Z})$ with $A\equiv 1 \pmod 3$, then

$$V_p\big(x^4+bx\big)=\begin{cases}\frac{1}{8}\big(5p+7+(-1)^{\frac{p-7}{12}}\cdot 6-4A\big) & \text{if } x^3\equiv 2b \pmod p \text{ is solvable},\\ \frac{1}{8}(5p+1+2A) & \text{if } x^3\equiv 2b \pmod p \text{ is unsolvable}.\end{cases} \tag{1.8}$$

If $p\equiv 1 \pmod{12}$ and $p=A^2+3B^2$ $(A,B\in\mathbb{Z})$, then

$$V_p\big(x^4+x\big)=\begin{cases}\frac{1}{8}\big(5p+9-(-1)^{\frac{p-1}{12}}\cdot 6\big) & \text{if } B\equiv 0 \pmod 3,\\ \frac{1}{8}(5p+3+6B) & \text{if } B\equiv 1 \pmod 3.\end{cases} \tag{1.9}$$

If $p\equiv 1, 9 \pmod{40}$ and so $p=s^2+5t^2$ for some $s,t\in\mathbb{Z}$, then

$$V_p\big(x^4-4x^2+4x\big)=\frac{5p+3}{8}+\frac{1-(-1)^t}{2}. \tag{1.10}$$

If $p\nmid ab$, $m\in\mathbb{Z}$ and $a^3m\equiv b^2 \pmod p$, then

$$V_p\big(x^4+ax^2+bx\big)=V_p\big(x^4+mx^2+m^2x\big). \tag{1.11}$$

If $p\equiv 7 \pmod{120}$, then

$$V_p\big(x^4-4x^2+4x\big)=\frac{1}{8}\big(3p-1+2\#E_p\big(x^3-12x-11\big)\big). \tag{1.12}$$

If $p\equiv 5 \pmod{12}$, then

$$V_p\big(x^4-3x^2+3x\big)=\frac{1}{8}\left(6p+6+2\left(\frac{2^{\frac{p-2}{3}}+1}{p}\right)-\#E_p\big(x^3-12x+20\big)\right). \tag{1.13}$$

If $p\equiv 5 \pmod{12}$ and $p=c^2+d^2$ with $2\mid d$, $c+d\equiv 1 \pmod 4$ and $c\equiv d \pmod 3$, then

$$V_p\big(x^4-3x^2+2x\big)=\frac{1}{8}(5p+3-2d). \tag{1.14}$$

2. On the value of $V_p(x^4+ax^2+bx)$ when p is prime

Let p be an odd prime and $ax\equiv c \pmod p$ with $a,c,x\in\mathbb{Z}$ and $p\nmid a$. Throughout this paper we use $(\frac{c/a}{p})$ to denote the Legendre symbol $(\frac{x}{p})$.

Let $a_1,a_2,a_3,a_4\in\mathbb{Z}$. Since $x^2\equiv x \pmod 2$ and $x^3\equiv x \pmod 3$ we see that

$$V_2\big(x^4+a_1x^3+a_2x^2+a_3x+a_4\big)=V_2\big((1+a_1+a_2+a_3)x+a_4\big)=\frac{3+(-1)^{a_1+a_2+a_3}}{2}$$

and

$$\begin{aligned}V_3\big(x^4+a_1x^3+a_2x^2+a_3x+a_4\big)&=V_3\big((1+a_2)x^2+(a_1+a_3)x\big)\\&=\begin{cases}1 & \text{if } a_2\equiv 2 \pmod 3 \text{ and } 3\mid(a_1+a_3),\\ 3 & \text{if } a_2\equiv 2 \pmod 3 \text{ and } 3\nmid(a_1+a_3),\\ 2 & \text{otherwise.}\end{cases}\end{aligned}$$

Let $p>3$ be a prime and $a,b\in\mathbb{Z}$. To determine the value of $V_p(x^4+ax^2+bx)$, we first deal with the simple case $b\equiv 0 \pmod p$.

Theorem 2.1. *Let p be an odd prime, $a\in\mathbb{Z}$ and $p\nmid a$. Then*

$$V_p\big(x^4+ax^2\big)=\left[\frac{3p+7-2(\frac{-a}{p})}{8}\right].$$

Proof. Clearly

$$\begin{aligned}&V_p\big(x^4+ax^2\big)\\&=\frac{p+1}{2}-\frac12\big|\big\{(x,y)\colon x^4+ax^2\equiv y^4+ay^2 \pmod p,\ x\neq y,\ x,y\in\big\{0,1,\dots,(p-1)/2\big\}\big\}\big|\\&=\frac{p+1}{2}-\frac12\big|\big\{(x,y)\colon x^2+y^2\equiv -a \pmod p,\ x\neq y,\ x,y\in\big\{0,1,\dots,(p-1)/2\big\}\big\}\big|\\&=\frac{p+1}{2}-\frac12\big|\big\{(x,y)\colon x^2+y^2+a\equiv 0 \pmod p,\ x,y\in\big\{0,1,\dots,(p-1)/2\big\}\big\}\big|\\&\quad+\frac12\big|\big\{(x,x)\colon 2x^2+a\equiv 0 \pmod p,\ x\in\big\{0,1,\dots,(p-1)/2\big\}\big\}\big|\\&=\frac{p+1}{2}+\frac14\left(1+\left(\frac{-2a}{p}\right)\right)-\frac12\sum_{\substack{x=0\\(\frac{-x^2-a}{p})=0,1}}^{(p-1)/2}1.\end{aligned}$$

Observe that

$$\sum_{\substack{x=0\\(\frac{-x^2-a}{p})=0,1}}^{(p-1)/2}1+\sum_{\substack{x=0\\(\frac{-x^2-a}{p})=-1}}^{(p-1)/2}1=\frac{p+1}{2}$$

and

$$\sum_{\substack{x=0\\(\frac{-x^2-a}{p})=0,1}}^{(p-1)/2} 1-\sum_{\substack{x=0\\(\frac{-x^2-a}{p})=-1}}^{(p-1)/2} 1=\sum_{x=0}^{(p-1)/2}\left(\frac{-x^2-a}{p}\right)+\frac{1+(\frac{-a}{p})}{2}.$$

We see that

$$\sum_{\substack{x=0\\(\frac{-x^2-a}{p})=0,1}}^{(p-1)/2} 1=\frac{1}{2}\left(\frac{p+1}{2}+\sum_{x=0}^{(p-1)/2}\left(\frac{-x^2-a}{p}\right)+\frac{1+(\frac{-a}{p})}{2}\right).$$

From [BEW, p. 58] we know that $\sum_{x=0}^{p-1}(\frac{x^2+a}{p})=-1$. Thus

$$\begin{aligned}\sum_{x=0}^{(p-1)/2}\left(\frac{-x^2-a}{p}\right)&=\left(\frac{-a}{p}\right)+\sum_{x=1}^{(p-1)/2}\left(\frac{-x^2-a}{p}\right)=\left(\frac{-a}{p}\right)+\frac{1}{2}\sum_{x=1}^{p-1}\left(\frac{-x^2-a}{p}\right)\\&=\left(\frac{-a}{p}\right)+\frac{1}{2}\left(\frac{-1}{p}\right)\left(\sum_{x=0}^{p-1}\left(\frac{x^2+a}{p}\right)-\left(\frac{a}{p}\right)\right)\\&=\left(\frac{-a}{p}\right)+\frac{1}{2}\left(\frac{-1}{p}\right)\left(-1-\left(\frac{a}{p}\right)\right)=\frac{1}{2}\left(\left(\frac{-a}{p}\right)-\left(\frac{-1}{p}\right)\right)\end{aligned}$$

and hence

$$\begin{aligned}\sum_{\substack{x=0\\(\frac{-x^2-a}{p})=0,1}}^{(p-1)/2} 1&=\frac{1}{2}\left(\frac{p+1}{2}+\frac{(\frac{-a}{p})-(\frac{-1}{p})}{2}+\frac{1+(\frac{-a}{p})}{2}\right)\\&=\frac{1}{4}\left(p+2-\left(\frac{-1}{p}\right)+2\left(\frac{-a}{p}\right)\right).\end{aligned}$$

Now combining the above, we obtain

$$\begin{aligned}V_p\big(x^4+ax^2\big)&=\frac{p+1}{2}+\frac{1+(\frac{-2a}{p})}{4}-\frac{1}{8}\left(p+2-\left(\frac{-1}{p}\right)+2\left(\frac{-a}{p}\right)\right)\\&=\frac{1}{8}\left(3p+4+\left(\frac{-1}{p}\right)+2\left(\frac{-a}{p}\right)\left(\left(\frac{2}{p}\right)-1\right)\right)=\left[\frac{3p+7-2(\frac{-a}{p})}{8}\right]\end{aligned}$$

as asserted. □

Let $D(a,b,c)$ be given by (1.4). Then clearly

$$\begin{aligned}a^2D(a,b,c)&=2ab^2\big(a^2+12c\big)^2+4c\big(2a^3-8ac+9b^2\big)^2\\&\quad-3b^2\big(a^2+12c\big)\big(2a^3-8ac+9b^2\big).\end{aligned}\tag{2.1}$$

From [Su3, Lemma 4.1] we have:

Lemma 2.1. *Let $p > 3$ be a prime, $a, b, c \in \mathbb{Z}$, $p \nmid b$ and $p \mid D(a,b,c)$. Then the congruence $(*)$ $x^3 + 2ax^2 + (a^2 - 4c)x - b^2 \equiv 0 \pmod p$ has three solutions. If $p \mid (a^2 + 12c)$, then $x \equiv -2a/3 \pmod p$ is the triple solution of $(*)$. If $p \nmid (a^2 + 12c)$, then the three solutions of $(*)$ are given by*

$$x \equiv \frac{9b^2 - 32ac}{a^2 + 12c},\ -\frac{2a^3 - 8ac + 9b^2}{2(a^2 + 12c)},\ -\frac{2a^3 - 8ac + 9b^2}{2(a^2 + 12c)} \pmod p.$$

Lemma 2.2. *Let $p > 3$ be a prime, $a, b \in \mathbb{Z}$, $p \nmid b$, and let R_p be a complete set of residues modulo p. If $\delta(a,b,p)$ is the number of those $c \in R_p$ such that $p \mid D(a,b,c)$ and the congruence $x^3 + 2ax^2 + (a^2 - 4c)x - b^2 \equiv 0 \pmod p$ has a quadratic nonresidue solution, then*

$$\delta(a,b,p) = \left| \left\{ y:\ 2y^3 + 2ay^2 + b^2 \equiv 0 \pmod p,\ \left(\frac{y}{p}\right) = -1,\ y \in R_p \right\} \right|.$$

Proof. We consider the following two cases.

Case 1. $8a^3 + 27b^2 \equiv 0 \pmod p$. In this case, for $c \in \mathbb{Z}$ we have

$$2a^3 - 8ac + 9b^2 \equiv 2a^3 - 8ac - \frac{8}{3}a^3 = -\frac{2a}{3}\big(a^2 + 12c\big) \pmod p.$$

This together with (2.1) yields

$$\begin{aligned} a^2 D(a,b,c) &\equiv \big(a^2 + 12c\big)^2 \left\{ 2ab^2 - 3b^2\left(-\frac{2a}{3}\right) + 4c \cdot \frac{4a^2}{9} \right\} \\ &\equiv \big(a^2 + 12c\big)^2 \left\{ 4a\left(-\frac{8}{27}a^3\right) + \frac{16}{9}a^2 c \right\} \\ &= \frac{16}{9}a^2\left(c - \frac{2}{3}a^2\right)\big(a^2 + 12c\big)^2 \pmod p. \end{aligned}$$

As $p \nmid b$ we have $p \nmid a$. Thus

$$p \mid D(a,b,c) \iff c \equiv \frac{2a^2}{3} \pmod p \quad \text{or} \quad c \equiv -\frac{a^2}{12} \pmod p.$$

Clearly

$$x^3 + 2ax^2 + \big(a^2 - 4c\big)x - b^2 \equiv \begin{cases} (x + \frac{2a}{3})^3 \pmod p & \text{if } c \equiv -\frac{a^2}{12} \pmod p, \\ (x - \frac{a}{3})^2 (x + \frac{8a}{3}) \pmod p & \text{if } c \equiv \frac{2a^2}{3} \pmod p. \end{cases}$$

Since $b^2 \equiv -\frac{8}{27}a^3 \pmod p$ we see that $-\frac{2a}{3}$ and $-\frac{8a}{3}$ are quadratic residues modulo p. Hence $\frac{a}{3}$ is a quadratic nonresidue modulo p if and only if $(\frac{-2}{p}) = -1$. Thus, by the above and the definition of $\delta(a, b, p)$ we obtain

$$\delta(a, b, p) = \frac{1}{2}\left(1 - \left(\frac{-2}{p}\right)\right).$$

On the other hand,

$$2y^3 + 2ay^2 + b^2 \equiv 2y^3 + 2ay^2 - \frac{8}{27}a^3 = 2\left(y - \frac{a}{3}\right)\left(y + \frac{2a}{3}\right)^2 \pmod p.$$

So we have

$$\left|\left\{y:\ 2y^3 + 2ay^2 + b^2 \equiv 0 \pmod p,\ \left(\frac{y}{p}\right) = -1,\ y \in R_p\right\}\right| = \frac{1}{2}\left(1 - \left(\frac{-2}{p}\right)\right) = \delta(a, b, p).$$

Case 2. $8a^3 + 27b^2 \not\equiv 0 \pmod p$. Let $c \in R_p$ be such that $p \mid D(a, b, c)$. We assert that $p \nmid (a^2 + 12c)$. If $p \mid (a^2 + 12c)$, by (2.1) we have $c(2a^3 - 8ac + 9b^2) \equiv (8a^3 + 27b^2)c/3 \equiv 0 \pmod p$. Thus $p \mid c$ and hence $p \mid a$. Applying (1.4) we see that $p \mid b$. This contradicts the assumption $p \nmid 8a^3 + 27b^2$. Thus the assertion is true.

Since $a^2 + 12c \not\equiv 0 \pmod p$, from Lemma 2.1 we know that the three solutions of the congruence $x^3 + 2ax^2 + (a^2 - 4c)x - b^2 \equiv 0 \pmod p$ are given by

$$x_1 \equiv \frac{9b^2 - 32ac}{a^2 + 12c} \pmod p \quad \text{and} \quad x_2 \equiv x_3 \equiv -\frac{2a^3 - 8ac + 9b^2}{2(a^2 + 12c)} \pmod p.$$

As $x_1x_2x_3 \equiv b^2 \pmod p$ we see that $(\frac{x_1}{p}) = 1$. Set

$$C = \left\{c:\ p \mid D(a, b, c),\ \left(\frac{-2(a^2 + 12c)(2a^3 - 8ac + 9b^2)}{p}\right) = -1,\ c \in R_p\right\}.$$

Then $\delta(a, b, p) = |C|$. It is easily seen that

$$\begin{aligned}
&2\left(-\frac{2a^3 - 8ac + 9b^2}{2(a^2 + 12c)}\right)^3 + 2a\left(-\frac{2a^3 - 8ac + 9b^2}{2(a^2 + 12c)}\right)^2 + b^2 \\
&\quad = \frac{8a^3 + 27b^2}{4(a^2 + 12c)^3}\left(256c^3 - 128a^2c^2 + 16\left(a^4 + 9ab^2\right)c - \left(4a^3 + 27b^2\right)b^2\right) \\
&\quad = \frac{8a^3 + 27b^2}{4(a^2 + 12c)^3}D(a, b, c).
\end{aligned}$$

Thus, if $c \in C$, then the congruence $2y^3 + 2ay^2 + b^2 \equiv 0 \pmod p$ has a quadratic nonresidue solution $y \equiv -(2a^3 - 8ac + 9b^2)/(2(a^2 + 12c)) \pmod p$. Conversely, if y is an integer such that $2y^3 + 2ay^2 + b^2 \equiv 0 \pmod p$ and $(\frac{y}{p}) = -1$, then $y \not\equiv \frac{a}{3} \pmod p$ since $p \nmid (8a^3 + 27b^2)$. Let $c \in R_p$ be given by $c \equiv -(2a^3 + 9b^2 + 2a^2y)/(24y - 8a) \pmod p$. Then clearly $y \equiv$

$-(2a^3-8ac+9b^2)/(2(a^2+12c))\pmod p$ and so $p \mid D(a,b,c)$ by the above. Thus $c \in C$. Now it is clear that there is a one-to-one correspondence between C and the set $S=\{y\colon\ 2y^3+2ay^2+b^2\equiv 0 \pmod p,\ (\frac{y}{p})=-1,\ y\in R_p\}$. This yields $\delta(a,b,p)=|C|=|S|$, which completes the proof. □

Now we can prove:

Theorem 2.2. *Let $p>3$ be a prime and $a,b\in\mathbb{Z}$ with $p\nmid b$. Then*

$$V_p\big(x^4+ax^2+bx\big)=\frac{1}{8}\left\{5p+3+4\delta(a,b,p)+\sum_{x=1}^{p-1}\left(\left(\frac{x}{p}\right)-1\right)\left(\frac{x(x+2a)^2-4b^2}{p}\right)\right\},$$

where

$$\delta(a,b,p)=\left|\left\{y\colon\ 2y^3+2ay^2+b^2\equiv 0 \pmod p,\ \left(\frac{y}{p}\right)=-1,\ y\in\{0,1,\ldots,p-1\}\right\}\right|.$$

Proof. For a polynomial $f(x)$ with integral coefficients we let $N_p(f(x))$ denote the number of solutions of the congruence $f(x)\equiv 0 \pmod p$. Let $R_p=\{0,1,\ldots,p-1\}$ and let $\alpha(a,b,p)$ denote the number of $c\in R_p$ such that $x^3+2ax^2+(a^2-4c)x-b^2\equiv 0 \pmod p$ has a quadratic nonresidue solution. Since

$$V_p\big(x^4+ax^2+bx\big)=\big|\big\{c\colon\ x^4+ax^2+bx+c\equiv 0 \pmod p \text{ is solvable},\ c\in R_p\big\}\big|,$$

we see that

$$\begin{aligned}
&p-V_p\big(x^4+ax^2+bx\big)\\
&\quad=\big|\big\{c\colon\ N_p\big(x^4+ax^2+bx+c\big)=0,\ c\in R_p\big\}\big|\\
&\quad=\big|\big\{c\colon\ p\nmid D(a,b,c),\ N_p\big(x^4+ax^2+bx+c\big)=0,\ c\in R_p\big\}\big| \quad \big(\text{by [Su3, Lemma 5.1]}\big)\\
&\quad=\big|\big\{c\colon\ p\nmid D(a,b,c),\ x^3+2ax^2+\big(a^2-4c\big)x-b^2\equiv 0 \pmod p\\
&\qquad\quad \text{has a quadratic nonresidue solution},\ c\in R_p\big\}\big| \quad \big(\text{by (1.5)}\big)\\
&\quad=\alpha(a,b,p)-\big|\big\{c\colon\ p\mid D(a,b,c),\ x^3+2ax^2+\big(a^2-4c\big)x-b^2\equiv 0 \pmod p\\
&\qquad\qquad\qquad \text{has a quadratic nonresidue solution},\ c\in R_p\big\}\big|\\
&\quad=\alpha(a,b,p)-\delta(a,b,p) \quad \text{(by Lemma 2.2).}
\end{aligned}$$

Thus,

$$V_p\big(x^4+ax^2+bx\big)=p+\delta(a,b,p)-\alpha(a,b,p). \tag{2.2}$$

If x_1,x_2,x_3 are distinct integers such that

$$x_1^2+2ax_1+a^2-\frac{b^2}{x_1}\equiv x_2^2+2ax_2+a^2-\frac{b^2}{x_2}\equiv x_3^2+2ax_3+a^2-\frac{b^2}{x_3} \pmod p,$$

then clearly $x_1x_2x_3 \equiv b^2 \pmod p$ by Vieta's theorem. This implies that $(\frac{x_1}{p}) = (\frac{x_2}{p}) = (\frac{x_3}{p}) = -1$ does not hold. From this we see that

$$\begin{aligned}
&\alpha(a,b,p)\\
&= \left|\left\{c:\ c \equiv \frac{x^3+2ax^2+a^2x-b^2}{4x} \pmod p,\ \left(\frac{x}{p}\right) = -1,\ c \in R_p\right\}\right|\\
&= \left|\left\{c:\ c \equiv x^2+2ax+a^2-\frac{b^2}{x} \pmod p,\ \left(\frac{x}{p}\right) = -1,\ c \in R_p\right\}\right|\\
&= \left|\left\{x:\ \left(\frac{x}{p}\right) = -1,\ x \in R_p\right\}\right| - \frac{1}{2}\left|\left\{(x_1,x_2):\ x_1^2+2ax_1+a^2-\frac{b^2}{x_1} \equiv x_2^2\right.\right.\\
&\qquad \left.\left. +2ax_2+a^2-\frac{b^2}{x_2} \pmod p,\ \left(\frac{x_1}{p}\right) = \left(\frac{x_2}{p}\right) = -1,\ x_1 \neq x_2,\ x_1,x_2 \in R_p\right\}\right|\\
&= \frac{p-1}{2} - \frac{1}{2}\left|\left\{(x_1,x_2):\ x_1+x_2+2a+\frac{b^2}{x_1x_2} \equiv 0 \pmod p,\right.\right.\\
&\qquad \left.\left. \left(\frac{x_1}{p}\right) = \left(\frac{x_2}{p}\right) = -1,\ x_1 \neq x_2,\ x_1,x_2 \in R_p\right\}\right|\\
&= \frac{p-1}{2} - \frac{1}{2}\left|\left\{(x_1,x_2):\ x_1x_2^2+(2a+x_1)x_1x_2+b^2 \equiv 0 \pmod p,\right.\right.\\
&\qquad \left.\left. \left(\frac{x_1}{p}\right) = \left(\frac{x_2}{p}\right) = -1,\ x_1 \neq x_2,\ x_1,x_2 \in R_p\right\}\right|\\
&= \frac{p-1}{2} - \frac{N-\delta(a,b,p)}{2},
\end{aligned}$$

where

$$N = \left|\left\{(x_1,x):\ x_1x^2+(2a+x_1)x_1x+b^2 \equiv 0 \pmod p,\ \left(\frac{x}{p}\right) = \left(\frac{x_1}{p}\right) = -1,\ x_1,x \in R_p\right\}\right|.$$

Thus, by (2.2) we have

$$\begin{aligned}
V_p\big(x^4+ax^2+bx\big) &= p+\delta(a,b,p) - \left(\frac{p-1}{2} - \frac{N-\delta(a,b,p)}{2}\right)\\
&= \frac{1}{2}\big(p+1+\delta(a,b,p)+N\big). \qquad (2.3)
\end{aligned}$$

Suppose $x_1 \in R_p$ and $(\frac{x_1}{p}) = -1$. Set $\Delta = (2a+x_1)^2x_1^2 - 4b^2x_1$. Then clearly $\Delta \not\equiv 0 \pmod p$ and

$$N_p\big(x_1x^2+(2a+x_1)x_1x+b^2\big) = 1+\left(\frac{\Delta}{p}\right).$$

If $(\frac{\Delta}{p})=1$, then the two solutions x_2, x_3 of the congruence $x_1x^2+(2a+x_1)x_1x+b^2\equiv 0 \pmod p$ satisfy the relation $x_2x_3\equiv \frac{b^2}{x_1} \pmod p$. Hence $(\frac{x_2}{p})(\frac{x_3}{p})=(\frac{x_1}{p})=-1$. So we have

$$\begin{aligned} N &= \left|\left\{x_1\colon \left(\frac{x_1}{p}\right)=-1,\ \left(\frac{\Delta}{p}\right)=1,\ x_1\in R_p\right\}\right| \\ &= \left|\left\{x\colon \left(\frac{x}{p}\right)=\left(\frac{x(x+2a)^2-4b^2}{p}\right)=-1,\ x\in R_p\right\}\right|. \end{aligned}$$

From this it is easy to see that

$$\sum_{x\in R_p}\left(1-\left(\frac{x}{p}\right)\right)\left(1-\left(\frac{x(x+2a)^2-4b^2}{p}\right)\right)=4N+1-\left(\frac{-1}{p}\right).$$

Thus, noting that $\sum_{x\in R_p}(\frac{x}{p})=0$ we obtain

$$\begin{aligned} N &= \frac{1}{4}\left\{\sum_{x\in R_p}\left(1-\left(\frac{x}{p}\right)\right)\left(1-\left(\frac{x(x+2a)^2-4b^2}{p}\right)\right)-1+\left(\frac{-1}{p}\right)\right\} \\ &= \frac{1}{4}\left\{p-1+\left(\frac{-1}{p}\right)-\sum_{x\in R_p}\left(\frac{x(x+2a)^2-4b^2}{p}\right)+\sum_{x\in R_p}\left(\frac{x}{p}\right)\left(\frac{x(x+2a)^2-4b^2}{p}\right)\right\} \\ &= \frac{1}{4}\left\{p-1+\sum_{x=1}^{p-1}\left(\left(\frac{x}{p}\right)-1\right)\left(\frac{x(x+2a)^2-4b^2}{p}\right)\right\}. \end{aligned}$$

This together with (2.3) gives the result. □

From Theorem 2.2 we have:

Theorem 2.3. *Let $p>3$ be a prime, $a,b\in\mathbb{Z}$ and $p\nmid ab$. Then $V_p(x^4+ax^2+bx)$ depends only on p and $b^2/a^3 \pmod p$. Moreover, if $k\in\mathbb{Z}$ and $k\equiv b^2/(2a^3) \pmod p$, then*

$$\begin{aligned} &V_p\big(x^4+ax^2+bx\big) \\ &= \frac{1}{8}\left\{5p+2+(-1)^{\frac{p-1}{2}}+4\delta(k,p)+\left(\frac{p}{3}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-(18k+3)x-(27k^2+18k+2)}{p}\right)\right. \\ &\qquad \left.-\left(\frac{p}{3}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-3k^2x+k^3(27k+2)}{p}\right)\right\}, \end{aligned}$$

where

$$\delta(k,p)=\left|\left\{x\colon x^3+4kx+8k^2\equiv 0 \pmod p,\ \left(\frac{x}{p}\right)=-1,\ x\in\{1,2,\ldots,p-1\}\right\}\right|. \quad (2.4)$$

Proof. Let $R_p=\{0,1,\ldots,p-1\}$ and let $\delta(a,b,p)$ be given as in Theorem 2.2. Since $(\frac{2ak}{p})=1$ we see that

$$\begin{aligned}\delta(a,b,p)&=\left|\left\{x:\ 2(2akx)^3+2a(2akx)^2+2a^3k\equiv 0\ (\mathrm{mod}\ p),\ \left(\frac{x}{p}\right)=-1,\ x\in R_p\right\}\right|\\&=\left|\left\{x:\ 8k^2x^3+4kx^2+1\equiv 0\ (\mathrm{mod}\ p),\ \left(\frac{x}{p}\right)=-1,\ x\in R_p\right\}\right|\\&=\delta(k,p).\end{aligned}$$

On the other hand, observing that $x(x+1)^2-k=\frac{1}{27}((3x+2)^3-3(3x+2)-27k-2)$ we obtain

$$\begin{aligned}&\sum_{x=1}^{p-1}\left(\frac{x(x+2a)^2-4b^2}{p}\right)\\&\quad=\sum_{x=1}^{p-1}\left(\frac{2ax(2ax+2a)^2-4b^2}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{k}{p}\right)\left(\frac{x(x+1)^2-k}{p}\right)\\&\quad=\sum_{x=0}^{p-1}\left(\frac{k}{p}\right)\left(\frac{x(x+1)^2-k}{p}\right)-\left(\frac{-1}{p}\right)\\&\quad=\left(\frac{k}{p}\right)\sum_{x=0}^{p-1}\left(\frac{27((3x+2)^3-3(3x+2)-27k-2)}{p}\right)-\left(\frac{-1}{p}\right)\\&\quad=\left(\frac{3k}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-3x-27k-2}{p}\right)-\left(\frac{-1}{p}\right)\\&\quad=\left(\frac{-3}{p}\right)\sum_{x=0}^{p-1}\left(\frac{-k^3x^3+3k^3x+k^3(27k+2)}{p}\right)-\left(\frac{-1}{p}\right)\\&\quad=\left(\frac{p}{3}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-3k^2x+k^3(27k+2)}{p}\right)-\left(\frac{-1}{p}\right).\end{aligned}$$

Also, since $y^3+y^2-2ky+k^2=-\frac{1}{27}((-3y-1)^3-3(6k+1)(-3y-1)-(27k^2+18k+2))$ we have

$$\begin{aligned}&\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\left(\frac{x(x+2a)^2-4b^2}{p}\right)\\&\quad=\sum_{x=1}^{p-1}\left(\frac{2ax}{p}\right)\left(\frac{2ax(2ax+2a)^2-4b^2}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\left(\frac{x(x+1)^2-k}{p}\right)\end{aligned}$$

$$= \sum_{x=1}^{p-1}\left(\frac{1+\frac{2}{x}+\frac{1}{x^2}-\frac{k}{x^3}}{p}\right) = \sum_{t=1}^{p-1}\left(\frac{1+2t+t^2-kt^3}{p}\right)$$

$$= \sum_{t=1}^{p-1}\left(\frac{-k^3t^3+k^2t^2+2k^2t+k^2}{p}\right) = \sum_{y=0}^{p-1}\left(\frac{y^3+y^2-2ky+k^2}{p}\right) - 1$$

$$= \sum_{y=0}^{p-1}\left(\frac{-3}{p}\right)\left(\frac{(-3y-1)^3-3(6k+1)(-3y-1)-(27k^2+18k+2)}{p}\right) - 1$$

$$= \left(\frac{p}{3}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-(18k+3)x-(27k^2+18k+2)}{p}\right) - 1.$$

Now putting all the above together with Theorem 2.2 yields the result. □

Corollary 2.1. *Let $p>3$ be a prime, $a,b\in\mathbb{Z}$ and $p\nmid ab$. If m is an integer such that $a^3m\equiv b^2 \pmod p$, then*

$$V_p\big(x^4+ax^2+bx\big) = V_p\big(x^4+mx^2+m^2x\big).$$

Proof. This is immediate from Theorem 2.3. □

For any prime $p>3$ let $\mathbb{F}_p$ be the field consisting of residue classes modulo p, and let $\#E_p(x^3-Ax-B)$ be the number of points on the elliptic curve $E_p\colon y^2=x^3-Ax-B$ over $\mathbb{F}_p$.

Corollary 2.2. *Let $p>3$ be a prime, and $k\in\mathbb{Z}$ with $p\nmid k$. Then*

$$\begin{aligned} &V_p\big(x^4+2kx^2+4k^2x\big)\\ &\quad= \frac{1}{8}\Big\{5p+2+(-1)^{\frac{p-1}{2}}+4\delta(k,p)+\left(\frac{p}{3}\right)\big\{\#E_p\big(x^3-(18k+3)x-27k^2-18k-2\big)\\ &\qquad -\#E_p\big(x^3-3k^2x+k^3(27k+2)\big)\big\}\Big\}, \end{aligned}$$

where $\delta(k,p)$ is given by (2.4).

Proof. Let $f(x)$ be a polynomial with integral coefficients, and $N_p(y^2=f(x))$ denote the number of solutions (x,y) of the congruence $y^2\equiv f(x) \pmod p$. It is easily seen that

$$N_p\big(y^2=f(x)\big) = \sum_{\substack{x=0\\(\frac{f(x)}{p})=0}}^{p-1} 1 + 2\sum_{\substack{x=0\\(\frac{f(x)}{p})=1}}^{p-1} 1 = p + \sum_{\substack{x=0\\(\frac{f(x)}{p})=1}}^{p-1} 1 - \sum_{\substack{x=0\\(\frac{f(x)}{p})=-1}}^{p-1} 1$$

$$= p+\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right).$$

Thus for $A, B \in \mathbb{Z}$ we have

$$\#E_p\big(x^3 - Ax - B\big) = 1 + N_p\big(y^2 = x^3 - Ax - B\big) = p + 1 + \sum_{x=0}^{p-1}\left(\frac{x^3 - Ax - B}{p}\right). \quad (2.5)$$

Now putting $a = 2k$ and $b = 4k^2$ in Theorem 2.3 and then applying the above we obtain the result. □

Remark 2.1. Let $p > 3$ be a prime, $k \in \mathbb{Z}$ and $p \nmid k$. By (2.5) we have

$$\begin{aligned}\#E_p\big(x^3 - 3k^2x + k^3(27k+2)\big) &= p + 1 + \sum_{x=0}^{p-1}\left(\frac{x^3 - 3k^2x + k^3(27k+2)}{p}\right)\\ &= p + 1 + \sum_{x=0}^{p-1}\left(\frac{(kx)^3 - 3k^2\cdot kx + k^3(27k+2)}{p}\right)\\ &= p + 1 + \left(\frac{k}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^3 - 3x + 27k + 2}{p}\right)\\ &= p + 1 + \left(\frac{k}{p}\right)\big(\#E_p\big(x^3 - 3x + 27k + 2\big) - p - 1\big).\end{aligned}$$

Hence

$$\#E_p\big(x^3 - 3k^2x + k^3(27k+2)\big) = \begin{cases}\#E_p(x^3 - 3x + 27k + 2) & \text{if } \left(\frac{k}{p}\right) = 1,\\ 2p + 2 - \#E_p(x^3 - 3x + 27k + 2) & \text{if } \left(\frac{k}{p}\right) = -1.\end{cases}$$

From Corollary 2.2 we have:

Corollary 2.3. *Let $p > 3$ be a prime, and $k \in \mathbb{Z}$ with $p \nmid k$. Then*

$$\begin{aligned}&\#E_p\big(x^3 - 3k^2x + k^3(27k+2)\big) - \#E_p\big(x^3 - (18k+3)x - \big(27k^2 + 18k + 2\big)\big)\\ &\quad\equiv 4\delta(k, p) + 2 - 2\left(\frac{-2}{p}\right) \pmod 8.\end{aligned}$$

Proof. From Corollary 2.2 we see that

$$\begin{aligned}&\#E_p\big(x^3 - 3k^2x + k^3(27k+2)\big) - \#E_p\big(x^3 - (18k+3)x - \big(27k^2 + 18k + 2\big)\big)\\ &\quad\equiv \left(\frac{p}{3}\right)\left(5p + 2 + \left(\frac{-1}{p}\right) + 4\delta(k, p)\right)\\ &\quad\equiv \left(\frac{p}{3}\right)\left(p - \left(\frac{-1}{p}\right) + 2\left(1 - \left(\frac{-1}{p}\right)\right) + 4\delta(k, p)\right)\\ &\quad\equiv 4\left(\frac{1}{4}\left(p - \left(\frac{-1}{p}\right)\right) + \frac{1}{2}\left(1 - \left(\frac{-1}{p}\right)\right) + \delta(k, p)\right)\end{aligned}$$

$$\equiv 4\left(\frac{1}{2}\left(1-\left(\frac{2}{p}\right)\right)+\frac{1}{2}\left(1-\left(\frac{-1}{p}\right)\right)+\delta(k,p)\right)$$
$$\equiv 4\left(\frac{1}{2}\left(1-\left(\frac{-2}{p}\right)\right)+\delta(k,p)\right) \pmod 8.$$

So the corollary is proved. □

Conjecture 2.1. Let $p>3$ be a prime, and $k\in\mathbb{Z}$ with $p\nmid k(27k+4)$. Then

$$\#E_p\big(x^3-(18k+3)x-\big(27k^2+18k+2\big)\big)\equiv 0 \pmod 3.$$

Theorem 2.4. *Let $p>3$ be a prime. If $a,b\in\mathbb{Z}$, $p\nmid ab$ and $8a^3\equiv -27b^2 \pmod p$, then*

$$V_p\big(x^4+ax^2+bx\big)=\left[\frac{5p+7}{8}\right].$$

Proof. Let $k\in\mathbb{Z}$ be such that $k\equiv\frac{b^2}{2a^3}\equiv-\frac{4}{27} \pmod p$. Then clearly

$$x^3+4kx+8k^2\equiv x^3-\frac{16}{27}x+\frac{8\cdot 16}{27^2}=\left(x-\frac{4}{9}\right)^2\left(x+\frac{8}{9}\right) \pmod p.$$

From this and (2.4) we see that

$$\delta(k,p)=\frac{1}{2}\left(1-\left(\frac{-2}{p}\right)\right).$$

On the other hand, setting $x=\frac{4}{9}y$ we find

$$x^3-3k^2x+k^3(27k+2)\equiv x^3-\frac{48}{27^2}x+\frac{128}{27^3}=\frac{64}{729}\left(y^3-\frac{1}{3}y+\frac{2}{27}\right)$$
$$\equiv\frac{64}{729}\big(y^3-(18k+3)y-\big(27k^2+18k+2\big)\big) \pmod p.$$

Thus,

$$\sum_{x=0}^{p-1}\left(\frac{x^3-3k^2x+k^3(27k+2)}{p}\right)=\sum_{x=0}^{p-1}\left(\frac{x^3-(18k+3)x-(27k^2+18k+2)}{p}\right).$$

Now applying the above and Theorem 2.3 we get

$$V_p\big(x^4+ax^2+bx\big)=\frac{1}{8}\left\{5p+2+\left(\frac{-1}{p}\right)+2\left(1-\left(\frac{-2}{p}\right)\right)\right\}$$
$$=\frac{1}{8}\left\{5p+4-2\left(\frac{-2}{p}\right)+\left(\frac{-1}{p}\right)\right\}=\left[\frac{5p+7}{8}\right].$$

This proves the corollary. □

Corollary 2.4. *Let $p > 3$ be a prime. Then*

$$V_p\big(x^4 - 6x^2 + 8x\big) = \left[\frac{5p+7}{8}\right].$$

Proof. Putting $a = -6$ and $b = 8$ in Theorem 2.4 we get the result. □

Theorem 2.5. *Let $p > 3$ be a prime, and $a, b \in \mathbb{Z}$ with $p \nmid b$. Then*

$$\left|V_p\big(x^4 + ax^2 + bx\big) - \frac{5p}{8}\right| \leqslant \frac{1}{2}\sqrt{p} + \frac{15}{8}.$$

Proof. If $p \nmid a$, letting $k \equiv b^2/(2a^3) \pmod p$ and then using Theorem 2.3 we see that

$$\begin{aligned}&\big|8V_p\big(x^4 + ax^2 + bx\big) - 5p\big| \\ &\quad\leqslant \left|2 + \left(\frac{-1}{p}\right) + 4\delta(k, p)\right| + \left|\sum_{x=0}^{p-1}\left(\frac{x^3 - (18k+3)x - (27k^2+18k+2)}{p}\right)\right| \\ &\qquad + \left|\sum_{x=0}^{p-1}\left(\frac{x^3 - 3k^2x + k^3(27k+2)}{p}\right)\right|.\end{aligned}$$

By Weil's estimate [BEW, p. 183] we have

$$\left|\sum_{x=0}^{p-1}\left(\frac{x^3 - (18k+3)x - (27k^2+18k+2)}{p}\right)\right| \leqslant 2\sqrt{p}$$

and

$$\left|\sum_{x=0}^{p-1}\left(\frac{x^3 - 3k^2x + k^3(27k+2)}{p}\right)\right| \leqslant 2\sqrt{p}.$$

As $0 \leqslant \delta(k, p) \leqslant 3$, applying the above we obtain

$$\left|V_p\big(x^4 + ax^2 + bx\big) - \frac{5p}{8}\right| \leqslant \frac{2+1+4\cdot 3}{8} + \frac{4\sqrt{p}}{8} = \frac{1}{2}\sqrt{p} + \frac{15}{8}.$$

If $p \mid a$, then $V_p(x^4 + ax^2 + bx) = V_p(x^4 + bx)$. It follows from Theorem 2.2 that

$$8V_p\big(x^4 + bx\big) - 5p = 3 + 4\delta(0, b, p) + \sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\left(\frac{x^3 - 4b^2}{p}\right) - \sum_{x=1}^{p-1}\left(\frac{x^3 - 4b^2}{p}\right).$$

Since

$$\sum_{x=1}^{p-1}\left(\frac{x^4-4b^2x}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{1-4b^2/x^3}{p}\right)=\sum_{t=1}^{p-1}\left(\frac{1-4b^2t^3}{p}\right)$$
$$=\left(\frac{-2b}{p}\right)\sum_{t=1}^{p-1}\left(\frac{-2b+8b^3t^3}{p}\right)=\left(\frac{-2b}{p}\right)\sum_{x=1}^{p-1}\left(\frac{x^3-2b}{p}\right)$$
$$=\left(\frac{-2b}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-2b}{p}\right)-1,$$

we see that

$$8V_p\big(x^4+bx\big)-5p$$
$$=2+\left(\frac{-1}{p}\right)+4\delta(0,b,p)+\left(\frac{-2b}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-2b}{p}\right)-\sum_{x=0}^{p-1}\left(\frac{x^3-4b^2}{p}\right). \tag{2.6}$$

Thus, using Weil's estimate we also get

$$\big|8V_p\big(x^4+ax^2+bx\big)-5p\big|\leqslant 2+1+4\cdot 3+2\sqrt{p}+2\sqrt{p}.$$

This yields the result and hence the proof is complete. □

Theorem 2.6. *Let $p\equiv 2 \pmod 3$ be an odd prime, $b\in\mathbb{Z}$ and $p\nmid b$. Then*

$$V_p\big(x^4+bx\big)=\left[\frac{5p+7}{8}\right].$$

Proof. Let

$$\delta(0,b,p)=\left|\left\{y\colon\ 2y^3+b^2\equiv 0 \pmod p,\ \left(\frac{y}{p}\right)=-1,\ y\in\{0,1,\ldots,p-1\}\right\}\right|.$$

Since $p\equiv 2 \pmod 3$ we know that the congruence $x^3\equiv t \pmod p$ has one and only one solution for any given integer t. So we have

$$\delta(0,b,p)=\frac{1}{2}\left(1-\left(\frac{-2}{p}\right)\right)$$

and

$$\sum_{x=0}^{p-1}\left(\frac{x^3+m}{p}\right)=\sum_{y=0}^{p-1}\left(\frac{y+m}{p}\right)=\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)=0\quad\text{for } m\in\mathbb{Z}. \tag{2.7}$$

Hence, by (2.6) we have

$$V_p\big(x^4+bx\big)=\frac{1}{8}\left\{5p+2+(-1)^{\frac{p-1}{2}}+2\left(1-\left(\frac{-2}{p}\right)\right)\right\}$$
$$=\frac{1}{8}\left(5p+4+\left(\frac{-1}{p}\right)-2\left(\frac{-2}{p}\right)\right)=\left[\frac{5p+7}{8}\right].$$

This completes the proof. □

Theorem 2.7. *Let $p\equiv 1 \pmod 3$ be a prime, $p=A^2+3B^2$ $(A,B\in\mathbb{Z})$, $A\equiv 1 \pmod 3$, $b\in\mathbb{Z}$ and $p\nmid b$.*

(i) *If $p\equiv 1 \pmod{12}$, then*

$$V_p\big(x^4+bx\big)=\begin{cases}\frac{1}{8}\big(5p+9-6(-1)^{\frac{p-1}{12}}\big) & \text{if } 2b \text{ is a cubic residue } (\mathrm{mod}\ p),\\ \frac{1}{8}(5p+3\pm 6B) & \text{if } (2b)^{\frac{p-1}{3}}\equiv\frac{1}{2}\big(-1\mp\frac{A}{B}\big)\ (\mathrm{mod}\ p).\end{cases}$$

(ii) *If $p\equiv 7 \pmod{12}$, then*

$$V_p\big(x^4+bx\big)=\begin{cases}\frac{1}{8}\big(5p+7+6(-1)^{\frac{p-7}{12}}-4A\big) & \text{if } 2b \text{ is a cubic residue } (\mathrm{mod}\ p),\\ \frac{1}{8}(5p+1+2A) & \text{if } 2b \text{ is a cubic nonresidue } (\mathrm{mod}\ p).\end{cases}$$

Proof. Let $a\in\mathbb{Z}$ be such that $p\nmid a$. The cubic Jacobsthal sums $\phi_3(a)$ and $\psi_3(a)$ are defined by

$$\phi_3(a)=\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\left(\frac{x^3+a}{p}\right)\quad\text{and}\quad\psi_3(a)=\sum_{x=1}^{p-1}\left(\frac{x^3+a}{p}\right).$$

It is clear that

$$\left(\frac{a}{p}\right)\phi_3\big(a^{-1}\big)=\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\left(\frac{ax^3+1}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{a+\frac{1}{x^3}}{p}\right)=\sum_{y=1}^{p-1}\left(\frac{y^3+a}{p}\right)=\psi_3(a).$$

From [BEW, Theorem 6.2.10, pp. 195, 196] we have

$$\phi_3(a)=\begin{cases}-1-2A & \text{if } a \text{ is a cubic residue } (\mathrm{mod}\ p),\\ -1+A\pm 3B & \text{if } a^{\frac{p-1}{3}}\equiv\frac{1}{2}\big(-1\pm\frac{A}{B}\big)\ (\mathrm{mod}\ p).\end{cases}\tag{2.8}$$

Hence

$$\left(\frac{a}{p}\right)\psi_3(a)=\phi_3\big(a^{-1}\big)=\begin{cases}-1-2A & \text{if } a \text{ is a cubic residue } (\mathrm{mod}\ p),\\ -1+A\pm 3B & \text{if } a^{\frac{p-1}{3}}\equiv\frac{1}{2}\big(-1\mp\frac{A}{B}\big)\ (\mathrm{mod}\ p).\end{cases}\tag{2.9}$$

Observe that $(4b^2)^{\frac{p-1}{3}}\equiv(2b)^{-\frac{p-1}{3}} \pmod p$. From (2.6) and the above we deduce that

$$\begin{aligned}
&8V_p\big(x^4+bx\big)-5p-3-4\delta(0,b,p)\\
&=\left(\frac{-2b}{p}\right)\psi_3(-2b)-\psi_3\big(-4b^2\big)=\phi_3\left(-\frac{1}{2b}\right)-\left(\frac{-4b^2}{p}\right)\phi_3\left(-\frac{1}{4b^2}\right)\\
&=\begin{cases}-1-2A-\left(\frac{-1}{p}\right)(-1-2A) & \text{if } 2b \text{ is a cubic residue (mod } p),\\ -1+A\pm 3B-\left(\frac{-1}{p}\right)(-1+A\mp 3B) & \text{if } (2b)^{\frac{p-1}{3}}\equiv\frac{1}{2}\big(-1\mp\frac{A}{B}\big) \text{ (mod } p).\end{cases}
\end{aligned}$$

This together with the fact

$$\begin{aligned}
\delta(0,b,p)&=\left|\left\{y\colon\ y^3\equiv-\frac{b^2}{2}\ (\mathrm{mod}\ p),\ \left(\frac{y}{p}\right)=-1,\ y\in\{0,1,\dots,p-1\}\right\}\right|\\
&=\begin{cases}3 & \text{if } \left(\frac{-2}{p}\right)=-1 \text{ and } 2b \text{ is a cubic residue (mod } p),\\ 0 & \text{otherwise,}\end{cases}\\
&=\begin{cases}3 & \text{if } p\equiv 7,13 \text{ (mod 24) and } 2b \text{ is a cubic residue (mod } p),\\ 0 & \text{otherwise}\end{cases}
\end{aligned}$$

yields the desired result. □

Let p be a prime of the form $3k+1$. Assume $p=A^2+3B^2$ and $4p=L^2+27M^2$ with $A,B,L,M\in\mathbb{Z}$. If 2 is a cubic residue of p, it is well known that $3\mid B$, $2\mid L$ and $2\mid M$ (see [IR, p. 119]). Thus

$$A=\pm\frac{L}{2},\qquad B=\pm\frac{3M}{2},\qquad L=\pm 2A,\qquad M=\pm\frac{2B}{3}. \tag{2.10}$$

If 2 is a cubic nonresidue of p, then $3\nmid AB$ and $2\nmid LM$. Thus we may choose the signs of A, B, L and M such that

$$L\equiv 1\pmod 3,\qquad M\equiv L\pmod 4\quad\text{and}\quad A\equiv B\equiv 1\pmod 3.$$

Now it is easy to check that

$$A=\frac{L-9M}{4},\qquad B=\frac{L+3M}{4},\quad L=A+3B \text{ and } M=\frac{B-A}{3}. \tag{2.11}$$

In [L1], Lehmer showed that $2^{\frac{p-1}{3}}\equiv(L+9M)/(L-9M)\pmod p$. (See also [IR, p. 137] and [Su1, Theorem 2.1].) Thus applying (2.11) we obtain

$$2^{\frac{p-1}{3}}\equiv\frac{(A+3B)+9(B-A)/3}{(A+3B)-9(B-A)/3}=\frac{-1+3B/A}{2}\equiv\frac{-1-A/B}{2}\pmod p. \tag{2.12}$$

Now from Theorem 2.7 and (2.12) we have:

Corollary 2.5. *Let $p\equiv 1$ (mod 6) be a prime and $p=A^2+3B^2$ with $A\equiv 1$ (mod 3) and $B\equiv 0,1$ (mod 3).*

(i) *If* $p\equiv 1 \pmod{12}$, *then*

$$V_p\big(x^4\pm x\big)=\begin{cases}\frac{1}{8}\big(5p+9-(-1)^{\frac{p-1}{12}}\cdot 6\big) & \text{if } B\equiv 0 \pmod 3,\\ \frac{1}{8}(5p+3+6B) & \text{if } B\equiv 1 \pmod 3.\end{cases}$$

(ii) *If* $p\equiv 7 \pmod{12}$, *then*

$$V_p\big(x^4\pm x\big)=\begin{cases}\frac{1}{8}\big(5p+7+(-1)^{\frac{p-7}{12}}\cdot 6-4A\big) & \text{if } B\equiv 0 \pmod 3,\\ \frac{1}{8}(5p+1+2A) & \text{if } B\equiv 1 \pmod 3.\end{cases}$$

Remark 2.2. Suppose that $p\equiv 1 \pmod 3$ is a prime and $p=A^2+3B^2$ with $A\equiv 1 \pmod 3$. If $2b$ is a cubic nonresidue of p, using (2.11) and [Su1, Theorem 2.1] we can determine the sign of B so that $(2b)^{\frac{p-1}{3}}\equiv\frac{1}{2}(-1-\frac{A}{B}) \pmod p$ and hence $V_p(x^4+bx)=\frac{1}{8}(5p+3+6B)$ for $p\equiv 1 \pmod{12}$.

Theorem 2.8. *Let p be a prime greater than 3. Let $a,b\in\mathbb{Z}$ be such that $p\nmid ab$ and $a^3\equiv -4b^2 \pmod p$ (for example, $a=-4$ and $b=4$). Let*

$$\delta(p)=\begin{cases}0 & \text{if } p\equiv 7,17,23,33 \pmod{40},\\ 1 & \text{if } p\equiv 3,13,27,31,37,39 \pmod{40},\\ 2 & \text{if } p\equiv 11,19 \pmod{40},\\ 1-(-1)^t & \text{if } p\equiv 1,9 \pmod{40} \text{ and } p=s^2+5t^2\ (s,t\in\mathbb{Z}),\\ 2+(-1)^t & \text{if } p\equiv 21,29 \pmod{40} \text{ and } p=s^2+5t^2\ (s,t\in\mathbb{Z}).\end{cases}$$

(i) *If* $p\equiv 1 \pmod 4$, *then*

$$V_p\big(x^4+ax^2+bx\big)=\frac{1}{8}\big(5p+3+4\delta(p)\big).$$

(ii) *If* $p\equiv 7 \pmod{12}$, *then*

$$V_p\big(x^4+ax^2+bx\big)=\frac{1}{8}\big(3p-1+4\delta(p)+2\#E_p\big(x^3-12x-11\big)\big).$$

(iii) *If* $p\equiv 11 \pmod{12}$, *then*

$$V_p\big(x^4+ax^2+bx\big)=\frac{1}{8}\big(7p+3+4\delta(p)-2\#E_p\big(x^3-12x-11\big)\big).$$

Proof. Let $k\in\mathbb{Z}$ be such that $k\equiv\frac{b^2}{2a^3}\equiv-\frac{1}{8} \pmod p$. Let $\delta(k,p)$ be given by (2.4) and $R_p=\{0,1,\ldots,p-1\}$. Then

$$\begin{aligned}\delta(k,p)&=\left|\left\{x\colon x^3-\frac{1}{2}x+\frac{1}{8}\equiv 0 \pmod p,\ \left(\frac{x}{p}\right)=-1,\ x\in R_p\right\}\right|\\ &=\left|\left\{x\colon \left(x-\frac{1}{2}\right)\left(x^2+\frac{1}{2}x-\frac{1}{4}\right)\equiv 0 \pmod p,\ \left(\frac{x}{p}\right)=-1,\ x\in R_p\right\}\right|\end{aligned}$$

$$= \frac{1-(\frac{2}{p})}{2} + \left|\left\{x\colon\ x^2+\frac{x}{2}-\frac{1}{4}\equiv 0 \pmod p,\ \left(\frac{x}{p}\right)=-1,\ x\in R_p\right\}\right|$$

$$= \frac{1-(\frac{2}{p})}{2} + \left|\left\{y\colon\ \left(\frac{y}{4}\right)^2+\frac{1}{2}\cdot\frac{y}{4}-\frac{1}{4}\equiv 0 \pmod p,\ \left(\frac{y}{p}\right)=-1,\ y\in R_p\right\}\right|$$

$$= \frac{1-(\frac{2}{p})}{2} + \left|\left\{y\colon\ y^2+2y-4\equiv 0 \pmod p,\ \left(\frac{y}{p}\right)=-1,\ y\in R_p\right\}\right|$$

$$= \frac{1-(\frac{2}{p})}{2} + \left|\left\{y\colon\ (y+1)^2\equiv 5 \pmod p,\ \left(\frac{y}{p}\right)=-1,\ y\in R_p\right\}\right|.$$

Thus, if $p\equiv 2,3 \pmod 5$, then $(\frac{5}{p})=-1$ and so $\delta(k,p)=\frac{1}{2}(1-(\frac{2}{p}))=\delta(p)$. If $p\equiv 11,19 \pmod{20}$, then

$$\left(\frac{-1+\sqrt{5}}{p}\right)\left(\frac{-1-\sqrt{5}}{p}\right)=\left(\frac{(-1+\sqrt{5})(-1-\sqrt{5})}{p}\right)=\left(\frac{-4}{p}\right)=-1$$

and so $\delta(k,p)=\frac{1}{2}(1-(\frac{2}{p}))+1=\delta(p)$. If $p\equiv 1,9 \pmod{20}$, we see that $(\frac{-1+\sqrt{5}}{p})(\frac{-1-\sqrt{5}}{p})=(\frac{-4}{p})=1$ and thus

$$\delta(k,p)=\frac{1-\left(\frac{2}{p}\right)}{2}+1-\left(\frac{1+\sqrt{5}}{p}\right)=\frac{3-\left(\frac{2}{p}\right)}{2}-\left(\frac{2}{p}\right)\left(\frac{(1+\sqrt{5})/2}{p}\right).$$

It is well known that $p=s^2+5t^2$ for some $s,t\in\mathbb{Z}$. From [Br] or [Su4, Remark 6.1] we know that $(\frac{(1+\sqrt{5})/2}{p})=(-1)^t$. Thus

$$\delta(k,p)=\frac{3-\left(\frac{2}{p}\right)}{2}-\left(\frac{2}{p}\right)(-1)^t=\delta(p).$$

Since $k\equiv -\frac{1}{8} \pmod p$, we see that

$$\sum_{x=0}^{p-1}\left(\frac{x^3-(18k+3)x-(27k^2+18k+2)}{p}\right)$$

$$=\sum_{x=0}^{p-1}\left(\frac{x^3-\frac{3}{4}x-\frac{11}{64}}{p}\right)=\sum_{y=0}^{p-1}\left(\frac{\frac{y^3}{4^3}-\frac{3}{4}\cdot\frac{y}{4}-\frac{11}{64}}{p}\right)=\sum_{y=0}^{p-1}\left(\frac{y^3-12y-11}{p}\right)$$

and

$$\sum_{x=0}^{p-1}\left(\frac{x^3-3k^2x+k^3(27k+2)}{p}\right)=\sum_{x=0}^{p-1}\left(\frac{x^3-\frac{3}{64}x+\frac{11}{64^2}}{p}\right)$$

$$= \sum_{y=0}^{p-1}\left(\frac{\left(-\frac{y}{16}\right)^3 - \frac{3}{64}\left(-\frac{y}{16}\right) + \frac{11}{64^2}}{p}\right)$$
$$= \sum_{y=0}^{p-1}\left(\frac{-1}{p}\right)\left(\frac{y^3 - 12y - 11}{p}\right).$$

Now combining the above with Theorem 2.3 and (2.5) we obtain

$$V_p\left(x^4 + ax^2 + bx\right)$$
$$= \frac{1}{8}\left\{5p + 2 + (-1)^{\frac{p-1}{2}} + 4\delta(p) + \left(\frac{p}{3}\right)\left(1 - (-1)^{\frac{p-1}{2}}\right)\sum_{y=0}^{p-1}\left(\frac{y^3 - 12y - 11}{p}\right)\right\}$$
$$= \frac{1}{8}\left\{5p + 2 + (-1)^{\frac{p-1}{2}} + 4\delta(p) + \left(\frac{p}{3}\right)\left(1 - (-1)^{\frac{p-1}{2}}\right)\left(\#E_p\left(x^3 - 12x - 11\right) - p - 1\right)\right\}.$$

This yields the result. □

Remark 2.3. If $p > 3$ is a prime of the form $4n + 3$, from Theorem 2.8 we deduce the following congruence

$$\#E_p\left(x^3 - 12x - 11\right) \equiv \begin{cases} 2 \pmod 4 & \text{if } p \equiv 3, 7 \pmod{20}, \\ 0 \pmod 4 & \text{if } p \equiv 11, 19 \pmod{20}. \end{cases}$$

If p is a prime greater than 5, we conjecture that

$$\#E_p\left(x^3 - 12x - 11\right) \equiv \begin{cases} 6 \pmod{12} & \text{if } p \equiv 3, 7 \pmod{20}, \\ 0 \pmod{12} & \text{if } p \equiv 1, 9, 11, 13, 17, 19 \pmod{20}. \end{cases}$$

Theorem 2.9. *Let p be a prime greater than 3. Let $a, b \in \mathbb{Z}$ be such that $p \nmid ab$ and $a^3 \equiv -3b^2 \pmod p$ (for example, $a = -3$ and $b = 3$). Let*

$$\delta(p) = \left|\left\{t\colon\ t^3 \equiv 2 \pmod p,\ \left(\frac{t+1}{p}\right) = -\left(\frac{2}{p}\right),\ t \in \{0, 1, \ldots, p-1\}\right\}\right|.$$

(i) *If $p \equiv 1 \pmod{12}$ and $p = A^2 + 3B^2$ ($A, B \in \mathbb{Z}$) with $A \equiv 1 \pmod 3$, then*

$$V_p\left(x^4 + ax^2 + bx\right)$$
$$= \begin{cases} \frac{1}{8}(6p + 4 + 4\delta(p) - 2A - \#E_p(x^3 - 12x + 20)) & \text{if } B \equiv 0 \pmod 3, \\ \frac{1}{8}(6p + 4 + A + 3B - \#E_p(x^3 - 12x + 20)) & \text{if } B \equiv 1 \pmod 3. \end{cases}$$

(ii) *If $p \equiv 5 \pmod{12}$, then*

$$V_p\left(x^4 + ax^2 + bx\right) = \frac{1}{8}\left(6p + 6 + 2\left(\frac{2^{\frac{p-2}{3}} + 1}{p}\right) - \#E_p\left(x^3 - 12x + 20\right)\right).$$

(iii) *If* $p\equiv 7 \pmod{12}$ *and* $p=A^2+3B^2$ $(A,B\in\mathbb{Z})$ *with* $A\equiv 1 \pmod 3$, *then*

$$V_p\big(x^4+ax^2+bx\big)=\begin{cases}\frac{1}{8}(4p+4\delta(p)-2A+\#E_p(x^3-12x+20)) & \text{if } B\equiv 0 \pmod 3,\\ \frac{1}{8}(4p+A+3B+\#E_p(x^3-12x+20)) & \text{if } B\equiv 1 \pmod 3.\end{cases}$$

(iv) *If* $p\equiv 11 \pmod{12}$, *then*

$$V_p\big(x^4+ax^2+bx\big)=\frac{1}{8}\left(4p+2+2\left(\frac{2^{\frac{p-2}{3}}+1}{p}\right)+\#E_p\big(x^3-12x+20\big)\right).$$

Proof. Let k be an integer such that $k\equiv \frac{b^2}{2a^3}\equiv -\frac{1}{6} \pmod p$. Set

$$S=\sum_{x=0}^{p-1}\left(\frac{x^3-(18k+3)x-27k^2-18k-2}{p}\right)$$

and

$$T=\sum_{x=0}^{p-1}\left(\frac{x^3-3k^2x+k^3(27k+2)}{p}\right).$$

If $p\equiv 2 \pmod 3$, then $S=\sum_{x=0}^{p-1}(\frac{x^3+\frac{1}{4}}{p})=0$ by (2.7). If $p\equiv 1 \pmod 3$ and $p=A^2+3B^2$ with $A\equiv 1 \pmod 3$ and $B\equiv 0,1 \pmod 3$, applying (2.8), (2.9) and (2.12) we see that

$$\begin{aligned}S-1&=\sum_{x=1}^{p-1}\left(\frac{x^3+\frac{1}{4}}{p}\right)=\psi_3\left(\frac{1}{4}\right)=\phi_3(4)\\&=\begin{cases}-1-2A & \text{if 2 is a cubic residue } (\mathrm{mod}\ p),\\ -1+A\pm 3B & \text{if } 2^{\frac{p-1}{3}}\equiv\frac{1}{2}\big(-1\mp\frac{A}{B}\big) \pmod p,\end{cases}\\&=\begin{cases}-1-2A & \text{if } B\equiv 0 \pmod 3,\\ -1+A+3B & \text{if } B\equiv 1 \pmod 3.\end{cases}\end{aligned}$$

We also have

$$\begin{aligned}T&=\sum_{x=0}^{p-1}\left(\frac{x^3-\frac{1}{12}x+\frac{5}{432}}{p}\right)=\sum_{y=0}^{p-1}\left(\frac{\frac{1}{12^3}y^3-\frac{1}{12^2}y+\frac{5}{432}}{p}\right)\\&=\sum_{y=0}^{p-1}\left(\frac{12^3}{p}\right)\left(\frac{y^3-12y+20}{p}\right)=\left(\frac{3}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-12x+20}{p}\right)\\&=(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)\big(\#E_p\big(x^3-12x+20\big)-p-1\big).\end{aligned}$$

Let $R_p=\{0,1,\ldots,p-1\}$. By (2.4) we have

$$\begin{aligned}\delta(k,p)&=\left|\left\{x\colon\ x^3-\frac{2}{3}x+\frac{2}{9}\equiv 0\ (\mathrm{mod}\ p),\ \left(\frac{x}{p}\right)=-1,\ x\in R_p\right\}\right|\\&=\left|\left\{y\colon\ -\frac{y^3}{3^3}-\frac{2}{3}\left(-\frac{y}{3}\right)+\frac{2}{9}\equiv 0\ (\mathrm{mod}\ p),\ \left(\frac{y}{p}\right)=-\left(\frac{-3}{p}\right),\ y\in R_p\right\}\right|\\&=\left|\left\{y\colon\ y^3-6y-6\equiv 0\ (\mathrm{mod}\ p),\ \left(\frac{y}{p}\right)=-\left(\frac{p}{3}\right),\ y\in R_p\right\}\right|.\end{aligned}$$

If $p\equiv 1\ (\mathrm{mod}\ 3)$, putting $a_1=0$ and $a_2=a_3=-6$ in [Su3, Theorem 4.5] we see that $x^3-6x-6\equiv 0\ (\mathrm{mod}\ p)$ has three solutions if and only if $x^3\equiv 2\ (\mathrm{mod}\ p)$ is solvable (that is $3\mid B$). Moreover, if $t^3\equiv 2\ (\mathrm{mod}\ p)$ for $t\in\mathbb{Z}$, then $x\equiv(t^2+2)/t\equiv t(t+1)\ (\mathrm{mod}\ p)$ is a solution of $x^3-6x-6\equiv 0\ (\mathrm{mod}\ p)$ with $(\frac{x}{p})=(\frac{2}{p})(\frac{t+1}{p})$. Thus, in view of [Su3, Lemma 2.2] we have $\delta(k,p)=\delta(p)$ or 0 according as $3\mid B$ or $3\nmid B$. If $p\equiv 2\ (\mathrm{mod}\ 3)$, from [Su3, Lemma 2.2] we know that the congruence $x^3-6x-6\equiv 0\ (\mathrm{mod}\ p)$ has the unique solution

$$x\equiv 2^{\frac{p+1}{3}}\left(2^{\frac{p-2}{3}}+1\right)\pmod p.$$

We thus have

$$\delta(k,p)=\frac{1}{2}\left(1+\left(\frac{2^{\frac{p-2}{3}}+1}{p}\right)\right).$$

From Theorem 2.3 we know that

$$V_p\left(x^4+ax^2+bx\right)=\frac{1}{8}\left\{5p+2+(-1)^{\frac{p-1}{2}}+4\delta(k,p)+\left(\frac{p}{3}\right)(S-T)\right\}.$$

Now putting all the above together we obtain the result. □

Lemma 2.3. *Let p be a prime greater than 3. Then*

$$\begin{aligned}&\#E_p\left(x^3-15x+22\right)-p-1\\&=\sum_{x=0}^{p-1}\left(\frac{x^3-15x+22}{p}\right)\\&=\begin{cases}-2A & \text{if } p\equiv 1\ (\mathrm{mod}\ 3) \text{ and } p=A^2+3B^2 \text{ with } A\equiv 1\ (\mathrm{mod}\ 3),\\ 0 & \text{if } p\equiv 2\ (\mathrm{mod}\ 3).\end{cases}\end{aligned}$$

Proof. From [W, p. 295] or [BEW, Exercise 21, p. 208] we know that

$$1+\sum_{n=0}^{p-1}\left(\frac{(n^2+4n+1)(n^2+2n)}{p}\right)=\begin{cases}-2A & \text{if } p\equiv 1\ (\mathrm{mod}\ 3),\\ 0 & \text{if } p\equiv 2\ (\mathrm{mod}\ 3).\end{cases}$$

As

$$\begin{aligned}
&1+\sum_{n=0}^{p-1}\left(\frac{(n^2+4n+1)(n^2+2n)}{p}\right)\\
&=1+\sum_{n=1}^{p-1}\left(\frac{n^4+6n^3+9n^2+2n}{p}\right)=1+\sum_{n=1}^{p-1}\left(\frac{1+\frac{6}{n}+\frac{9}{n^2}+\frac{2}{n^3}}{p}\right)\\
&=\sum_{x=0}^{p-1}\left(\frac{1+6x+9x^2+2x^3}{p}\right)=\sum_{x=0}^{p-1}\left(\frac{4+24x+36x^2+8x^3}{p}\right)\\
&=\sum_{x=0}^{p-1}\left(\frac{x^3+9x^2+12x+4}{p}\right)=\sum_{x=0}^{p-1}\left(\frac{(x-3)^3+9(x-3)^2+12(x-3)+4}{p}\right)\\
&=\sum_{x=0}^{p-1}\left(\frac{x^3-15x+22}{p}\right),
\end{aligned}$$

by the above and (2.5) we obtain the result. □

Theorem 2.10. *Let p be a prime greater than 3. Let $a,b\in\mathbb{Z}$, $p\nmid ab$ and $4a^3\equiv -27b^2 \pmod p$ (for example, $a=-3$ and $b=2$).*

(i) *If $p\equiv 1 \pmod{12}$ and $p=A^2+3B^2=c^2+d^2$ with $2\mid d$, $c+d\equiv 1 \pmod 4$ and $A\equiv 1 \pmod 3$, then*

$$V_p\left(x^4+ax^2+bx\right)=\begin{cases}\frac{1}{8}(5p+3+4\delta(p)-2A-2c) & \text{if } 3\mid c,\\ \frac{1}{8}(5p+3+4\delta(p)-2A+2c) & \text{if } 3\mid d,\end{cases}$$

where

$$\delta(p)=\begin{cases}1 & \text{if } p\equiv 13 \pmod{24},\\ 0 & \text{if } p\equiv 1 \pmod{24} \text{ and } B\equiv d \pmod 8,\\ 2 & \text{if } p\equiv 1 \pmod{24} \text{ and } B\not\equiv d \pmod 8.\end{cases}$$

(ii) *If $p\equiv 5 \pmod{12}$ and $p=c^2+d^2$ with $2\mid d$, $c+d\equiv 1 \pmod 4$ and $c\equiv d \pmod 3$, then*

$$V_p\left(x^4+ax^2+bx\right)=\frac{1}{8}(5p+3-2d).$$

(iii) *If $p\equiv 7 \pmod{12}$ and $p=A^2+3B^2$ with $A\equiv 1 \pmod 3$, then*

$$V_p\left(x^4+ax^2+bx\right)=\frac{1}{8}(5p+1-2A).$$

(iv) *If* $p\equiv 11 \pmod{12}$, *then*

$$V_p\big(x^4+ax^2+bx\big)=\begin{cases}\frac{5p+1}{8}+\frac{1}{2}\big(1-\big(\frac{3^{\frac{p+1}{4}}+1}{p}\big)\big) & \text{if } p\equiv 11 \pmod{24},\\ \frac{5}{8}(p+1) & \text{if } p\equiv 23 \pmod{24}.\end{cases}$$

Proof. Let $k\in\mathbb{Z}$ be such that $k\equiv \frac{b^2}{2a^3}\equiv -\frac{2}{27} \pmod p$. Let $\delta(k,p)$ be given by (2.4) and $R_p=\{0,1,\ldots,p-1\}$. Then

$$\begin{aligned}\delta(k,p)&=\left|\left\{x\colon\ x^3-\frac{8}{27}x+\frac{32}{27^2}\equiv 0 \pmod p,\ \left(\frac{x}{p}\right)=-1,\ x\in R_p\right\}\right|\\&=\left|\left\{x\colon\ \left(x-\frac{4}{9}\right)\left(\left(x+\frac{2}{9}\right)^2-\frac{4}{27}\right)\equiv 0 \pmod p,\ \left(\frac{x}{p}\right)=-1,\ x\in R_p\right\}\right|\\&=\left|\left\{x\colon\ \left(x+\frac{2}{9}\right)^2\equiv\frac{4}{27} \pmod p,\ \left(\frac{x}{p}\right)=-1,\ x\in R_p\right\}\right|\\&=\left|\left\{x\colon\ \left(-\frac{2y}{9}+\frac{2}{9}\right)^2\equiv\frac{4}{27} \pmod p,\ \left(\frac{-2y}{p}\right)=-1,\ y\in R_p\right\}\right|\\&=\left|\left\{y\colon\ (y-1)^2\equiv 3 \pmod p,\ \left(\frac{y}{p}\right)=-\left(\frac{-2}{p}\right),\ y\in R_p\right\}\right|.\end{aligned}$$

Thus, if $p\equiv 5,7 \pmod{12}$, then $(\frac{3}{p})=-1$ and so $\delta(k,p)=0$. If $p\equiv 13,23 \pmod{24}$, then

$$\left(\frac{1+\sqrt{3}}{p}\right)\left(\frac{1-\sqrt{3}}{p}\right)=\left(\frac{(1+\sqrt{3})(1-\sqrt{3})}{p}\right)=\left(\frac{-2}{p}\right)=-1$$

and so $\delta(k,p)=1$. If $p\equiv 1,11 \pmod{24}$, we see that

$$\left(\frac{1+\sqrt{3}}{p}\right)\left(\frac{1-\sqrt{3}}{p}\right)=\left(\frac{-2}{p}\right)=1$$

and thus $\delta(k,p)=1-(\frac{1+\sqrt{3}}{p})$. When $p\equiv 11 \pmod{24}$, we have $(3^{\frac{p+1}{4}})^2\equiv 3 \pmod p$ and so $\delta(k,p)=1-(\frac{1+3^{(p+1)/4}}{p})$.

When $p\equiv 1 \pmod{24}$, then $p=A^2+3B^2=c^2+d^2$ with $B\equiv d\equiv 0 \pmod 4$. It is well known that $2^{\frac{p-1}{4}}\equiv(-1)^{\frac{d}{4}} \pmod p$. Also,

$$\left(\frac{1+\sqrt{3}}{p}\right)=\big(1+\sqrt{3}\big)^{\frac{p-1}{2}}=2^{\frac{p-1}{4}}\big(2+\sqrt{3}\big)^{\frac{p-1}{4}}\equiv(-1)^{\frac{d}{4}}\big(2+\sqrt{3}\big)^{\frac{p-1}{4}} \pmod p.$$

From [L2] or [Su4, Theorem 8.1] (with $m=4$, $n=2$, $d=3$ and $k=8$) we have

$$\big(2+\sqrt{3}\big)^{\frac{p-1}{4}}\equiv(-1)^{\frac{B}{4}} \pmod p. \tag{2.13}$$

Thus

$$\left(\frac{1+\sqrt{3}}{p}\right)=(-1)^{\frac{B-d}{4}}. \tag{2.14}$$

Hence $\delta(k,p)=1-(\frac{1+\sqrt{3}}{p})=\delta(p)$.

Using Lemma 2.3 we see that

$$\begin{aligned}
&\sum_{x=0}^{p-1}\left(\frac{x^3-(18k+3)x-27k^2-18k-2}{p}\right)\\
&\quad=\sum_{x=0}^{p-1}\left(\frac{x^3-\frac{5}{3}x-\frac{22}{27}}{p}\right)=\sum_{y=0}^{p-1}\left(\frac{\left(-\frac{y}{3}\right)^3-\frac{5}{3}\cdot\left(-\frac{y}{3}\right)-\frac{22}{27}}{p}\right)\\
&\quad=\left(\frac{-3}{p}\right)\sum_{y=0}^{p-1}\left(\frac{y^3-15y+22}{p}\right)\\
&\quad=\begin{cases}-2A & \text{if } p\equiv 1 \pmod 3 \text{ and } p=A^2+3B^2 \text{ with } A\equiv 1 \pmod 3,\\ 0 & \text{if } p\equiv 2 \pmod 3.\end{cases}
\end{aligned}$$

On the other hand,

$$\begin{aligned}
&\sum_{x=0}^{p-1}\left(\frac{x^3-3k^2x+k^3(27k+2)}{p}\right)\\
&\quad=\sum_{x=0}^{p-1}\left(\frac{x^3-\frac{12}{27^2}x}{p}\right)=\sum_{y=0}^{p-1}\left(\frac{\frac{1}{27^3}y^3-\frac{12}{27^2}\cdot\frac{y}{27}}{p}\right)=\sum_{y=0}^{p-1}\left(\frac{27^3}{p}\right)\left(\frac{y^3-12y}{p}\right)\\
&\quad=\left(\frac{3}{p}\right)\sum_{x=1}^{p-1}\left(\frac{x^3-12x}{p}\right)=\left(\frac{3}{p}\right)\phi_2(-12),
\end{aligned}$$

where

$$\phi_2(D)=\sum_{x=1}^{p-1}\left(\frac{x^3+Dx}{p}\right)\quad\text{for } D\in\mathbb{Z}.$$

Suppose $p\nmid D$. If $p\equiv 3 \pmod 4$, we see that

$$\phi_2(D)=\sum_{y=1}^{p-1}\left(\frac{(-y)^3+D(-y)}{p}\right)=\left(\frac{-1}{p}\right)\phi_2(D)\quad\text{and so}\quad\phi_2(D)=0. \tag{2.15}$$

If $p\equiv 1 \pmod 4$, we may write $p=c^2+d^2$ $(c,d\in\mathbb{Z})$ with $2\mid d$ and $c+d\equiv 1 \pmod 4$. Since $p\equiv 1 \pmod 8 \Leftrightarrow 4\mid d \Leftrightarrow c\equiv 1 \pmod 4$ we see that $-(-1)^{\frac{p-1}{4}}c\equiv -1 \pmod 4$. Hence by [BEW, Theorem 6.2.9, p. 195] we have

$$\phi_2(-D)=\begin{cases}\pm 2\big(-(-1)^{\frac{p-1}{4}}c\big) & \text{if } (-D)^{\frac{p-1}{4}}\equiv \pm 1 \pmod p,\\ \pm 2d & \text{if } (-D)^{\frac{p-1}{4}}\equiv \pm\dfrac{d}{-(-1)^{\frac{p-1}{4}}c} \pmod p.\end{cases}$$

Thus

$$\phi_2(-D)=\begin{cases}\mp 2c & \text{if } D^{\frac{p-1}{4}}\equiv \pm 1 \pmod p,\\ \mp 2d & \text{if } D^{\frac{p-1}{4}}\equiv \pm\frac{d}{c} \pmod p.\end{cases} \tag{2.16}$$

Since

$$12^{\frac{p-1}{4}}=(-3)^{\frac{p-1}{4}}(-1)^{\frac{p-1}{4}}2^{\frac{p-1}{2}}\equiv (-3)^{\frac{p-1}{4}}(-1)^{\frac{p-1}{4}}\left(\frac{2}{p}\right)=(-3)^{\frac{p-1}{4}} \pmod p,$$

by (2.16) we have

$$\phi_2(-12)=\begin{cases}\mp 2c & \text{if } (-3)^{\frac{p-1}{4}}\equiv \pm 1 \pmod p,\\ \mp 2d & \text{if } (-3)^{\frac{p-1}{4}}\equiv \pm\frac{d}{c} \pmod p.\end{cases}$$

From [Su2, Theorem 2.2 and Example 2.1] we know that

$$(-3)^{\frac{p-1}{4}}\equiv\begin{cases}1 \pmod p & \text{if } 3\mid d,\\ -1 \pmod p & \text{if } 3\mid c,\\ \pm\frac{d}{c} \pmod p & \text{if } c\equiv\mp d \pmod 3.\end{cases}$$

Thus

$$\phi_2(-12)=\begin{cases}-2c & \text{if } 3\mid d,\\ 2c & \text{if } 3\mid c,\\ \pm 2d & \text{if } c\equiv\pm d \pmod 3.\end{cases} \tag{2.17}$$

From the above we see that

$$\left(\frac{p}{3}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-3k^2x+k^3(27k+2)}{p}\right)=\left(\frac{p}{3}\right)\left(\frac{3}{p}\right)\phi_2(-12)=(-1)^{\frac{p-1}{2}}\phi_2(-12)$$
$$=\begin{cases}0 & \text{if } p\equiv 3 \pmod 4,\\ 2c & \text{if } p\equiv 1 \pmod 4 \text{ and } 3\mid c,\\ -2c & \text{if } p\equiv 1 \pmod 4 \text{ and } 3\mid d,\\ \pm 2d & \text{if } p\equiv 1 \pmod 4 \text{ and } c\equiv\pm d \pmod 3.\end{cases}$$

By Theorem 2.3,

$$V_p\big(x^4+ax^2+bx\big) = \frac{1}{8}\Bigg\{5p+2+(-1)^{\frac{p-1}{2}}+4\delta(k,p)+\left(\frac{p}{3}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-(18k+3)x-(27k^2+18k+2)}{p}\right) - \left(\frac{p}{3}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-3k^2x+k^3(27k+2)}{p}\right)\Bigg\}.$$

Now putting all the above together we deduce the result. □

3. The values of $V_m(x^2)$ and $V_m(x^3+a_1x^2+a_2x+a_3)$

For any positive integer m and polynomial $f(x)$ with integral coefficients let

$$S_m\big(f(x)\big)=\big\{c:\ f(x)\equiv c\ (\mathrm{mod}\ m)\ \text{is solvable},\ c\in\{0,1,\ldots,m-1\}\big\}.$$

Then clearly $V_m(f(x))=|S_m(f(x))|$.

Theorem 3.1. *Suppose that $f(x)$ is a polynomial with integral coefficients and $m=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ is the prime decomposition of m. Then*

$$V_m\big(f(x)\big)=V_{p_1^{\alpha_1}}\big(f(x)\big)\cdots V_{p_r^{\alpha_r}}\big(f(x)\big).$$

Proof. For $a,c\in\{0,1,\ldots,m-1\}$ and $i\in\{1,2,\ldots,r\}$ let $a_i,c_i\in\{0,1,\ldots,p_i^{\alpha_i}-1\}$ be given by $a\equiv a_i\ (\mathrm{mod}\ p_i^{\alpha_i})$ and $c\equiv c_i\ (\mathrm{mod}\ p_i^{\alpha_i})$. It is clear that

$$\begin{aligned} f(a)\equiv c\ \ (\mathrm{mod}\ m) &\iff f(a)\equiv c\ \ \big(\mathrm{mod}\ p_i^{\alpha_i}\big)\ (i=1,2,\ldots,r),\\ &\iff f(a)\equiv c_i\ \ \big(\mathrm{mod}\ p_i^{\alpha_i}\big)\ (i=1,2,\ldots,r),\\ &\iff f(a_i)\equiv c_i\ \ \big(\mathrm{mod}\ p_i^{\alpha_i}\big)\ (i=1,2,\ldots,r).\end{aligned}$$

Thus

$$c\in S_m\big(f(x)\big)\iff c_i\in S_{p_i^{\alpha_i}}\big(f(x)\big)\quad(i=1,2,\ldots,r).$$

Now applying the Chinese Remainder Theorem we see that

$$V_m\big(f(x)\big)=\big|S_m\big(f(x)\big)\big|=\prod_{i=1}^{r}\big|S_{p_i^{\alpha_i}}\big(f(x)\big)\big|=\prod_{i=1}^{r}V_{p_i^{\alpha_i}}\big(f(x)\big).$$

This proves the theorem. □

Theorem 3.2. *Let $p>1$ be odd. Then p is a prime if and only if $0^2,1^2,2^2,\ldots,(\frac{p-1}{2})^2$ are pairwise distinct modulo p. Namely, p is a prime if and only if $V_p(x^2)=\frac{p+1}{2}$.*

Proof. If p is a prime, it is well known that $0^2, 1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ are pairwise distinct modulo p. If p is composite, then there are two odd numbers d and d' such that $1 < d' \leqslant d < p$ and $dd' = p$. Set $x_1 = (d + d')/2$ and $x_2 = (d - d')/2$. Then clearly $x_1, x_2 \in \{0, 1, \ldots, p-1\}$ and $x_1^2 - x_2^2 = (x_1 + x_2)(x_1 - x_2) = dd' = p$. Let $y_1 = \min\{x_1, p - x_1\}$ and $y_2 = \min\{x_2, p - x_2\}$. Then $y_1, y_2 \in \{0, 1, \ldots, (p-1)/2\}$ and $y_1^2 \equiv x_1^2 \equiv x_2^2 \equiv y_2^2 \pmod p$. Since $x_1 + x_2 = d$ and $x_1 - x_2 = d'$ we see that $x_1 \neq x_2, p - x_2$ and so $y_1 \neq y_2$. Thus $0^2, 1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ are not pairwise distinct modulo p and hence $V_p(x^2) < \frac{p+1}{2}$. This proves the theorem. □

For a given polynomial $f(x)$ we let $f'(x)$ denote the derivative of $f(x)$. If p is a prime and $f(x_0) \equiv 0 \pmod{p^{\alpha-1}}$ for $x_0 \in \mathbb{Z}$ and $\alpha > 1$, using the binomial theorem one can easily derive that

$$f\big(x_0 + sp^{\alpha-1}\big) \equiv f(x_0) + sp^{\alpha-1} f'(x_0) \pmod{p^\alpha} \quad \text{for } s \in \mathbb{Z}.$$

From this we deduce:

Lemma 3.1. *Suppose that p is a prime and $f(x)$ is a polynomial with integral coefficients. If there is an integer x_0 such that $f(x_0) \equiv 0 \pmod p$ and $p \nmid f'(x_0)$, then for any positive integer α the congruence $f(x) \equiv 0 \pmod{p^\alpha}$ is solvable.*

Lemma 3.1 can be deduced from Hensel's lemma. See [HW, Theorem 123, pp. 96, 97] and [R, Theorem 4.14].

Theorem 3.3. *If $m > 1$ is odd and $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is the prime decomposition of m, then*

$$V_m\big(x^2\big) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} + p_i + 2 + (p_i - 1)(1 - (-1)^{\alpha_i})/2}{2(p_i + 1)}.$$

Proof. Let p be an odd prime and let $\alpha \geqslant 2$ be a positive integer. We assert that

$$V_{p^\alpha}\big(x^2\big) = V_{p^{\alpha-2}}\big(x^2\big) + \frac{p^{\alpha-1}(p-1)}{2}. \tag{3.1}$$

If $c \in \mathbb{Z}$ and $p \nmid c$, it follows from Lemma 3.1 that $x^2 \equiv c \pmod{p^\alpha}$ is solvable if and only if $x^2 \equiv c \pmod p$ is solvable. Suppose $S_p(x^2) = \{0, a_1, a_2, \ldots, a_{(p-1)/2}\}$. We then have

$$\big\{c\colon\ c \in S_{p^\alpha}\big(x^2\big),\ p \nmid c\big\} = \big\{a_i + sp\colon\ i = 1, 2, \ldots, (p-1)/2,\ s = 0, 1, \ldots, p^{\alpha-1} - 1\big\}$$

and thus

$$\big|\big\{c\colon\ c \in S_{p^\alpha}\big(x^2\big),\ p \nmid c\big\}\big| = p^{\alpha-1}(p-1)/2.$$

If $c \in S_{p^\alpha}(x^2)$ and $p \mid c$, then $x^2 \equiv c \pmod{p^\alpha}$ for some $x \in \mathbb{Z}$. As $p \mid c$ we have $p \mid x$ and so $p^2 \mid c$. For $t \in \mathbb{Z}$, clearly $x^2 \equiv p^2 t \pmod{p^\alpha}$ is solvable if and only if $y^2 \equiv t \pmod{p^{\alpha-2}}$ is solvable. Thus

$$\big|\big\{c\colon\ c \in S_{p^\alpha}\big(x^2\big),\ p \mid c\big\}\big| = \big|\big\{t\colon\ t \in S_{p^{\alpha-2}}\big(x^2\big)\big\}\big| = V_{p^{\alpha-2}}\big(x^2\big).$$

Hence

$$V_{p^\alpha}(x^2) = \big|\{c:\ c \in S_{p^\alpha}(x^2),\ p \mid c\}\big| + \big|\{c:\ c \in S_{p^\alpha}(x^2),\ p \nmid c\}\big|$$
$$= V_{p^{\alpha-2}}(x^2) + p^{\alpha-1}(p-1)/2.$$

This proves the assertion (3.1).

Observe that $V_p(x^2) = \frac{p+1}{2}$ and $V_1(x^2) = 1$. Using (3.1) we see that

$$V_{p^{2\beta+1}}(x^2) = \frac{p-1}{2}\sum_{s=1}^{\beta} p^{2s} + V_p(x^2) = \frac{p^{2\beta+2}+2p+1}{2(p+1)}$$

and

$$V_{p^{2\beta}}(x^2) = \frac{p-1}{2}\sum_{s=1}^{\beta} p^{2s-1} + V_1(x^2) = \frac{p^{2\beta+1}+p+2}{2(p+1)}.$$

Now combining this with Theorem 3.1 gives the result. □

Theorem 3.4. *Let a_1, a_2, a_3 and $m > 1$ be integers with $\gcd(m, 6(a_1^2 - 3a_2)) = 1$. If $m = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ is the prime decomposition of m, then*

$$V_m(x^3 + a_1x^2 + a_2x + a_3) = m\prod_{i=1}^{r}\frac{2p_i + \left(\frac{p_i}{3}\right)}{3p_i}.$$

Proof. Let p be a prime divisor of m. Let $c \in \mathbb{Z}$ and $f(x) = x^3 + a_1x^2 + a_2x + a_3 - c$. According to [Su3], the discriminant of $f(x)$ is given by $D(f(x)) = -\frac{1}{27}(b^2 - 4a)$, where $a = (a_1^2 - 3a_2)^3$ and $b = -2a_1^3 + 9a_1a_2 - 27(a_3 - c)$. Now we claim that $f(x) \equiv 0 \pmod p$ is solvable if and only if $f(x) \equiv 0 \pmod{p^\alpha}$ is solvable. Clearly $f(x) \equiv 0 \pmod{p^\alpha}$ is solvable implies $f(x) \equiv 0 \pmod p$ is solvable.

If $p \nmid D(f(x))$, it is well known that $f(x) \equiv 0 \pmod p$ has no multiple solutions. Hence, if $f(x_0) \equiv 0 \pmod p$ for some integer x_0, then $f'(x_0) \not\equiv 0 \pmod p$. Now, using Lemma 3.1 we see that $f(x) \equiv 0 \pmod p$ is solvable implies $f(x) \equiv 0 \pmod{p^\alpha}$ is solvable.

If $p \mid D(f(x))$, we set

$$x_0 = -a_1 + \frac{a_1a_2 - 9(a_3 - c)}{a_1^2 - 3a_2} = \frac{1}{3}\left(\frac{b}{a_1^2 - 3a_2} - a_1\right).$$

From [Su3, Lemma 4.1] we know that $x \equiv x_0 \pmod p$ is a solution of the congruence $f(x) \equiv 0 \pmod p$. As $b^2 \equiv 4a \pmod p$ we see that

$$f'(x_0) = 3x_0^2 + 2a_1x_0 + a_2 = \frac{1}{3}\left(\frac{b}{a_1^2 - 3a_2} - a_1\right)^2 + \frac{2a_1}{3}\left(\frac{b}{a_1^2 - 3a_2} - a_1\right) + a_2$$
$$= \frac{1}{3(a_1^2 - 3a_2)^2}\left(b^2 - \left(a_1^2 - 3a_2\right)^3\right) \equiv a_1^2 - 3a_2 \not\equiv 0 \pmod p.$$

Thus $f(x)\equiv 0 \pmod{p^\alpha}$ is solvable by Lemma 3.1.

By the above, the assertion is true. Suppose

$$S_p\big(x^3+a_1x^2+a_2x+a_3\big)=\{c_1,c_2,\ldots,c_n\}.$$

Then we must have

$$S_{p^\alpha}\big(x^3+a_1x^2+a_2x+a_3\big)=\big\{c_i+tp\colon\ i=1,2,\ldots,n,\ t=0,1,\ldots,p^{\alpha-1}-1\big\}.$$

Hence applying (1.1) we get

$$V_{p^\alpha}\big(x^3+a_1x^2+a_2x+a_3\big)=p^{\alpha-1}n=p^{\alpha-1}V_p\big(x^3+a_1x^2+a_2x+a_3\big)=p^{\alpha-1}\frac{2p+(\frac{p}{3})}{3}.$$

This together with Theorem 3.1 yields the result. □

Theorem 3.5. *Let $m,a_1,a_2,a_3\in\mathbb{Z}$ with $m>3$ and $\gcd(m,6(a_1^2-3a_2))=1$. Then m is a prime if and only if $V_m(x^3+a_1x^2+a_2x+a_3)=(2m+(\frac{m}{3}))/3$.*

Proof. If m is a prime, the result is true by (1.1). Now suppose $m=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ is composite, where $p_1,\ldots,p_r$ are distinct primes. If $r=1$, then $\alpha_1>1$. It follows from Theorem 3.4 that

$$V_m\big(x^3+a_1x^2+a_2x+a_3\big)=m\left(\frac{2}{3}+\frac{1}{3p_1}\left(\frac{p_1}{3}\right)\right)\neq\frac{1}{3}\left(2m+\left(\frac{m}{3}\right)\right).$$

So the result holds in the case $r=1$.

Now suppose $r>1$. Since $p_i\geqslant 5$ we see that

$$\prod_{i=1}^{r}\left(\frac{2}{3}+\frac{1}{3p_i}\left(\frac{p_i}{3}\right)\right)\leqslant\prod_{i=1}^{r}\left(\frac{2}{3}+\frac{1}{15}\right)=\left(\frac{11}{15}\right)^r<0.54\left(\frac{11}{15}\right)^{r-2}<\frac{2}{3}+\frac{1}{3m}\left(\frac{m}{3}\right).$$

Thus, by Theorem 3.4,

$$V_m\big(x^3+a_1x^2+a_2x+a_3\big)=m\prod_{i=1}^{r}\left(\frac{2}{3}+\frac{1}{3p_i}\left(\frac{p_i}{3}\right)\right)<\frac{2m+(\frac{m}{3})}{3}.$$

This completes the proof. □

Corollary 3.1. *Let $p\geqslant 5$ be an integer such that $p\equiv\pm1 \pmod 6$. Then p is a prime if and only if $V_p(x^3-x)=(2p+(\frac{p}{3}))/3$.*

References

[BEW] B.C. Berndt, R.J. Evans, K.S. Williams, Gauss and Jacobi Sums, Wiley, New York, 1998.
[BSD] B.J. Birch, H.P.F. Swinnerton-Dyer, Note on a problem of Chowla, Acta Arith. 5 (1959) 417–423.
[Br] J. Brandler, Residuacity properties of real quadratic units, J. Number Theory 5 (1973) 271–287.
[HW] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, fifth ed., Oxford Univ. Press, 1981, p. 97.
[IR] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, Springer, New York, 1982.

[K] R. Kantor, Über die Anzahl inkongruenter Werte ganzer, rationaler Funktionen, Monatsh. Math. Phys. 26 (1915) 24–39.
[L1] E. Lehmer, On Euler's criterion, J. Aust. Math. Soc. 1 (1) (1959/1961) 64–70.
[L2] E. Lehmer, On the quartic character of quadratic units, J. Reine Angew. Math. 268/269 (1974) 294–301.
[Leo] P.A. Leonard, On factoring quartics (mod p), J. Number Theory 1 (1969) 113–115.
[MW1] K. McCann, K.S. Williams, On the residues of a cubic polynomial (mod p), Canad. Math. Bull. 10 (1967) 29–38.
[MW2] K. McCann, K.S. Williams, The distribution of the residues of a quartic polynomial, Glasg. Math. J. 8 (1967) 67–88.
[R] K.H. Rosen, Elementary Number Theory and Its Applications, fourth ed., Addison–Wesley, Reading, MA, 2000.
[Sk] T. Skolem, The general congruence of 4th degree modulo p, p prime, Norsk Mat. Tidsskr. 34 (1952) 73–80.
[St] R.D. von Sterneck, Über die Anzahl inkongruenter Werte, die eine ganze Funktion dritten Grades annimmt, Sitzungsber. Akad. Wiss. Wien (2A) 114 (1908) 711–717.
[Su1] Z.H. Sun, On the theory of cubic residues and nonresidues, Acta Arith. 84 (1998) 291–335.
[Su2] Z.H. Sun, Supplements to the theory of quartic residues, Acta Arith. 97 (2001) 361–377.
[Su3] Z.H. Sun, Cubic and quartic congruences modulo a prime, J. Number Theory 102 (2003) 41–89.
[Su4] Z.H. Sun, Quartic residues and binary quadratic forms, J. Number Theory 113 (2005) 10–52.
[W] K.S. Williams, Evaluation of character sums connected with elliptic curves, Proc. Amer. Math. Soc. 73 (1979) 291–299.